PERSPECTIVE

Can bitcoins be the new oil currency?

Liz Bossley, CEO, Consilience Energy Advisory Group (CEAG)

What would Winston Churchill and Franklin D Roosevelt (FDR) make of cryptocurrency?

Churchill presided in 1925 over Britain's return to the gold standard after WWI, before it was finally abandoned again in 1931. FDR took the US off the gold standard in 1933. Today, while politicians debate a return to the gold standard, the market is trying to take responsibility for currency out of the hands of governments and put into the control of disparate groups of individuals by creating cryptocurrencies.

Cryptocurrencies are one evolutionary step on from the current system of 'fiat' currencies, such as Dollars, Euros and Sterling. These traditional notes have no intrinsic value, but their relative worth depends on the amount of currency put into circulation by governments and on international perceptions of the economic performance of the country issuing them.

It requires a willing suspension of disbelief to contemplate the market mutation that has brought cryptocurrencies into existence.

What are bitcoins?

Bitcoins are just one example of a cryptocurrency. Cryptocurrency is to paper money what email was to the postal system. It is a means of exchange between any two individuals anywhere in the world without the need for, or the cost of, a banking intermediary. There is no government controlling the supply and exchange of bitcoins through quantitative easing, interest or FOREX controls or any other intervention.

Like greenhouse gas (GHG) emissions permits, bitcoins represent a string of numbers in a computer, but unlike GHG permits bitcoins are not created or held in a centralised registry. Nor are they retired when they have served the purpose for which they were created, in this case profit.

Each bitcoin is a chain of digital signatures verifying the time and order of transactions on a vast network of interconnected nodes. A block chain is a distributed ledger, each containing a record of all transactions that have taken place across all nodes since the first one was created in 2009.

The process involves two separate chains.

- The *transaction chain* verifies transactions across the network and ensures that a party initiating a bitcoin payment has the coinage available to spend. It does this by verifying the transactional history of every bitcoin user;
- The *block chain* arranges bitcoin transactions in chronological order, ie giving them an identifying timestamp. Any node connected to the network can group together a set of unconfirmed transactions, which is called a block. Because different nodes can suggest different blocks, there needs to be a system to decide which block becomes the accepted next link in the block chain.

Creating, or 'mining', bitcoins requires only central processing unit (CPU) time and electricity to solve a mathematical puzzle to create a block chain. The person who solves the block first is given a reward for doing so in the form of spendable bitcoins.

Every time another 21,000 blocks have been added to the system the reward for finding a new block will be halved.

Because a bit block is a 'distributed consensus' of a series of transactions, in theory, bitcoins cannot be forged. As each user everywhere has a record of the timing and order of all deals done to date, an illegitimate coin would stick out like a sore thumb.

Bitcoin transactions are conducted in a very public digital arena and yet the identity of the traders remains anonymous. Each transaction has a unique signature created using a public and a private key. The public encryption key is the digital address of the person to whom the bitcoins are being sent. This can only be decrypted by using the private key of the person who is the owner of that public key. This like confirming that the password is known without actually revealing the password.

Who is using cryptocurrency?

At the time of writing there are thought to be 15.5mn bitcoins in circulation. One bitcoin is worth about $460, or £320, or €410. Ultimately, the mathematicians state confidently that there will be an upper limit of about 21mn bitcoins that can be mined. But that will not limit the size of the market because it will also be possible to deal in fractions of bitcoins.

While one of the early movers in the market has been the black economy it would be unsurprising if President Rouhani of Iran was flirting with cryptocurrencies to circumvent the continuing American prohibition on Iran using the US dollar, despite the nuclear deal that came into force in January of this year. Cryptocurrency could be a big step along the road to de-politicising the oil market by replacing the dollar as the dominant petrocurrency.

So, am I planning to convert my own modest funds into bitcoins? Absolutely not. One of the first things I learned as a trader is not to trade a commodity until you understand it. Until I have a firm grasp on the mathematics underlying the puzzles that have to be solved to mine bitcoins, with apologies to that great stateswoman – Marilyn Munroe – diamonds are this girl's best friend. ●

Additional research by James Walmsley